Cyber Defense Through Common Sense

Michigan Association of Airport Executives

February 17th, 2016

J.A. Lewis

lewisja@aim.com

www.michiganccdn.com www.cyberdefensetrainingsystems.com www.cyberdefenseresearch.com

Where this Information Originates

- **Organic & Research Based**

  Independent contractors, research and testing on isolated and live production networks

- **Cyber Defense Exercises**

  Hacking competitions and pre-compromised networks with industry and L.E. oversight! (March 12th Davenport University G.R., April 16th Baker Flint)

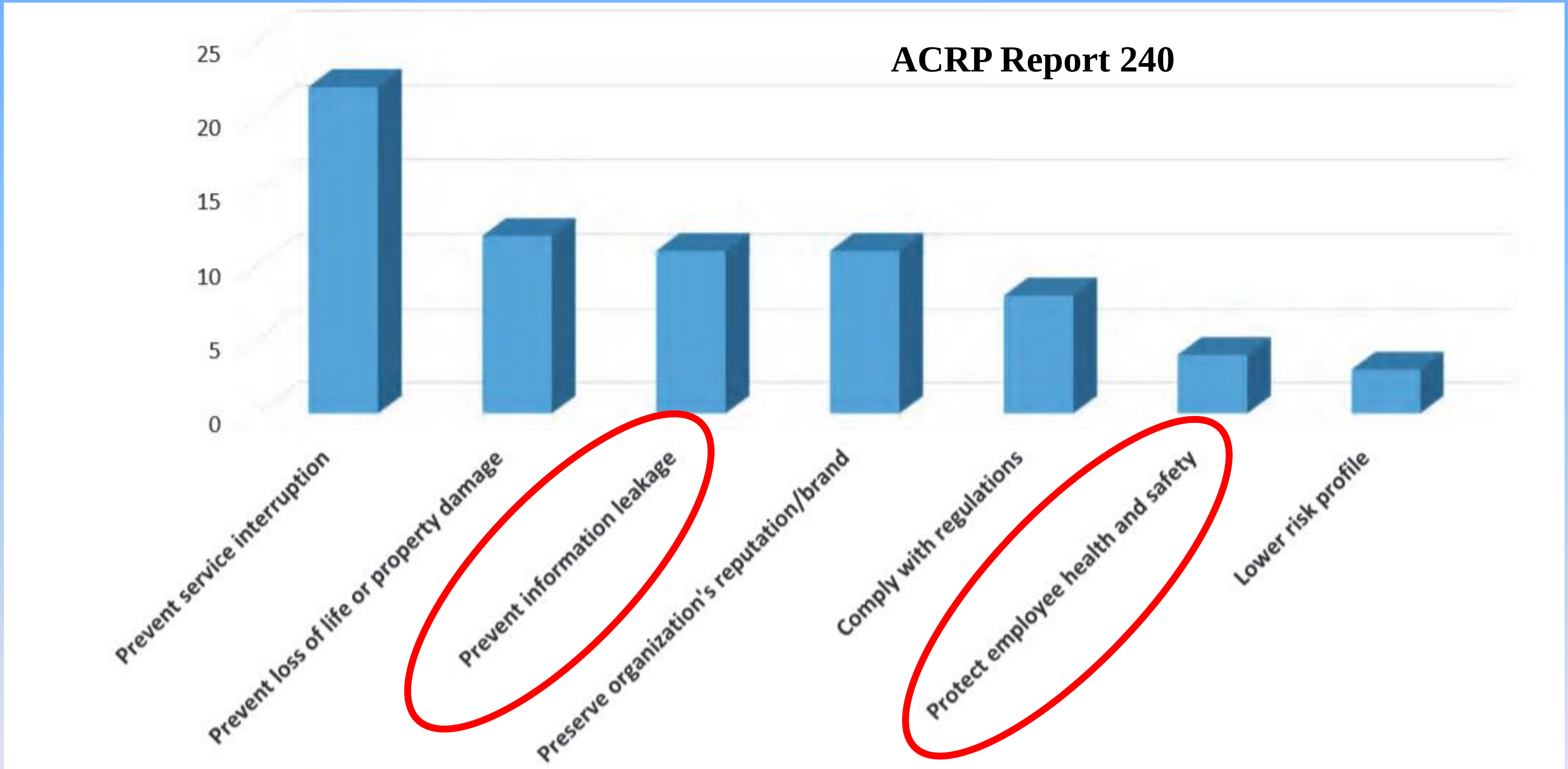
- **Technology and Engineering Oriented College Students**

  Cutting edge skills, not afraid to try anything on someone else's network

- **Industry and Law Enforcement**

  Industry experiences, L.E. raids and investigations

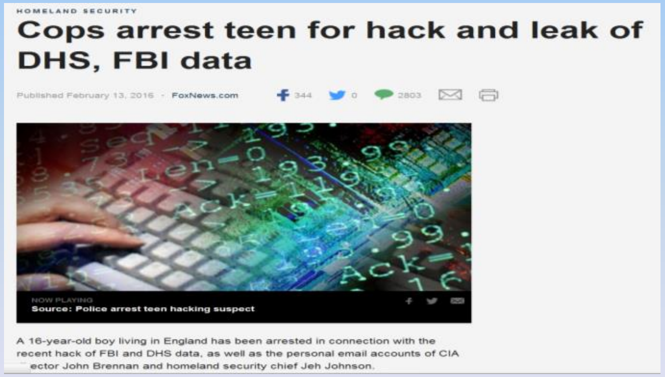
Why the Concern?



Source: 27 of 55 (49%) survey respondents.

Consider the Following

- What is cyberspace?
- What is the number one product produced in this country?
- What is security?
- Why are systems so inherently insecure?
- What skill level does someone need to aid in the compromising of a network or system?



HOMELAND SECURITY

Cops arrest teen for hack and leak of DHS, FBI data

Published February 13, 2016 · FoxNews.com

Source: Police arrest teen hacking suspect

A 16-year-old boy living in England has been arrested in connection with the recent hack of FBI and DHS data, as well as the personal email accounts of CIA ector John Brennan and homeland security chief Jeh Johnson.

- What effect has technology had upon law, culture, society, economics and security?

Challenges

- More than 25,000 Internet related crimes are reported each month to the Internet Crime Complaint Center

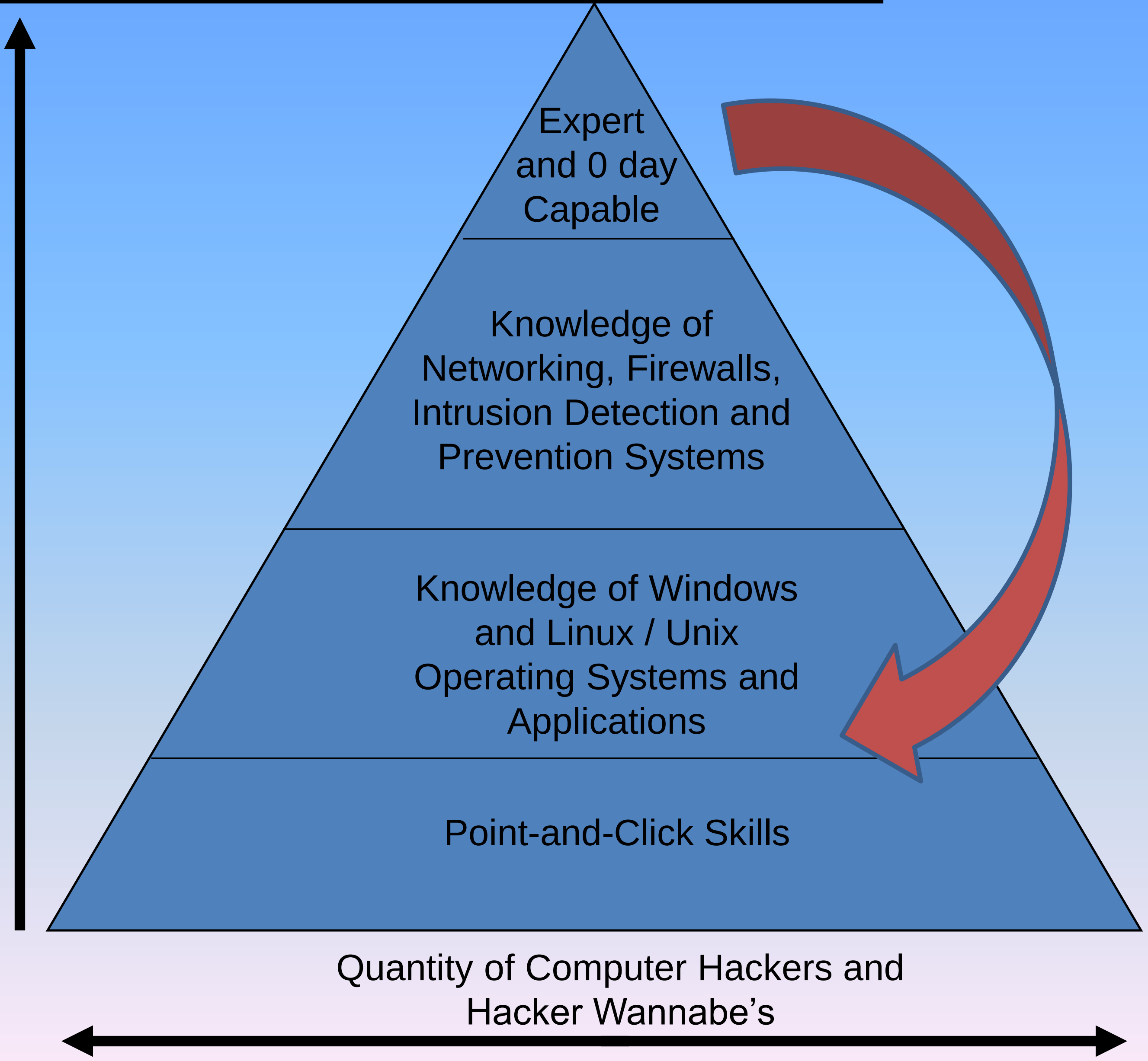
- According to the 2012 Cyber Security Watch Survey (Table 1),
  - 72% of cyber crimes go unreported
  - 42% of known cases involved copying information to a mobile device such as a USB drive (U.S. Secret Service, Software Engineering Institute, CERT and Deloitte, 2010)

  - **So, we do them ourselves before the public finds them**!

The Attacker Skill Level Pyramid

High Skills in Code and Programming

Low and Skills in Code and Programming



Expert and 0 day Capable

Knowledge of Networking, Firewalls, Intrusion Detection and Prevention Systems

Knowledge of Windows and Linux / Unix Operating Systems and Applications

Point-and-Click Skills

Quantity of Computer Hackers and Hacker Wannabe’s

J.A. Lewis 2007
Cyber Defense Training Systems, LLC

Consider Who Would be the Best at Providing Internal Confidential Information?

Trained agents?

Computer hackers?

The person who doesn’t realize they are providing sensitive information?

Social Media??? Cell Phone Contents???

Study Info

- A study conducted at 10,470 companies in Europe and North and South America revealed that 25% of the newly circulated worms in 2010 were claimed to be able to spread via USB device

  (U.S. Secret Service, Software Engineering Institute, CERT and Deloitte, 2010)

Planet of the APPs

- Estimated that the 1Q of 2012 there were 419 million mobile phones sold to end users world wide
- Practically all mobile devices radiate a signal
- Mobile apps are highly vulnerable!
- App Store (for apps that work on Apple devices) and Google Play (for apps that work on Android devices). They are believed to be the two largest stores with over 800,000 apps apiece

Reported Cases of Intrusion without Immediate Detection

- In October of 2006 a drug-related investigation at a private residence revealed a thumb drive that contained classified documents from the Los Alamos National Laboratory. The residence was that of a former subcontractor to the laboratory (U.S Department of Energy, 2006)

- In 2008 a USB device was inserted into a Pentagon network computer that was connected to a military network in the Middle East. The USB device was infected with malicious software that spread to numerous internal networks to where it was understood to have gained access to parts of the network that were classified as secret. (U.S. Secret Service, Software Engineering Institute, CERT and Deloitte, 2010)

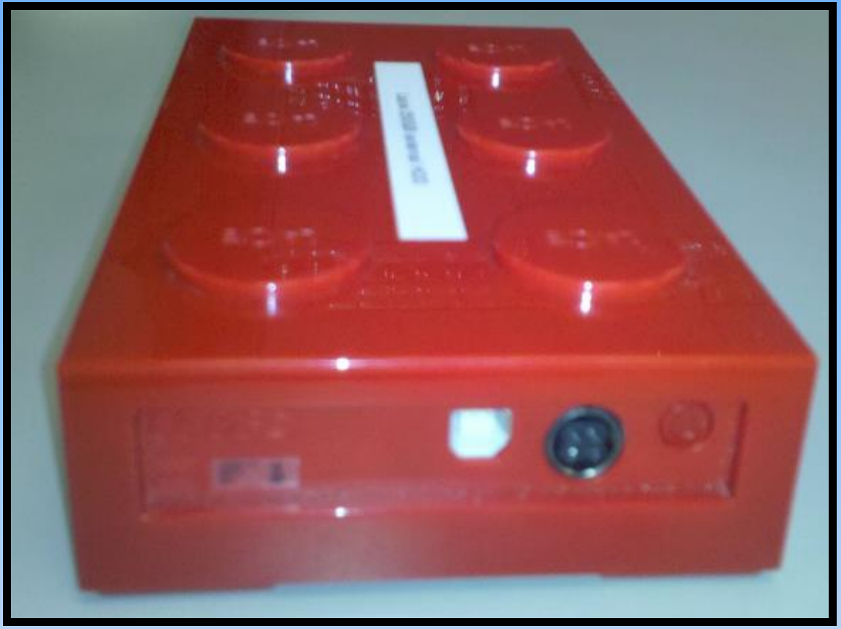
Reported Cases of Intrusion without Immediate Detection

- In 2009 a military contractor had detected programs of a questionable nature in their computer network. Further investigation discovered that the computer networks of the military contractor “had been infiltrated by an unknown malware, classified as a Remote-Access Tool or RAT. The RAT provided hackers unauthorized access to critical information stored on the network. (Coleman, 2008)
- Another case of cyber-espionage that has been reported as being the world’s largest was reported by the Threat Research department of McAfee, a U.S. based security firm. A report from McAfee titled “Revealed: Operation Shady RAT, An investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years”. (Alperovitch, 2011). This report indicated that “virtually everyone is falling prey to these intrusions, regardless of whether they are the United Nations, a multinational Fortune 100 company, a small, non-profit think tank, a national Olympic team, or even an unfortunate computer security firm”. (Alperovitch, 2011).

Simple Vector Attacks

- Hidden thumb drives are extremely effective
  - Physically small
  - Capacities from 4 to 128 Gigabytes.
  - May contain many millions of pages of text, drawings or software.
  - Can be altered to conceal their appearance for purposes of:
    - Egress of sensitive information – Auto load programs!
    - Ingress of malicious software – Auto load programs!
    - Initial front line officer assessment: Approximately 35% discovery of concealed devices

Actual Cases

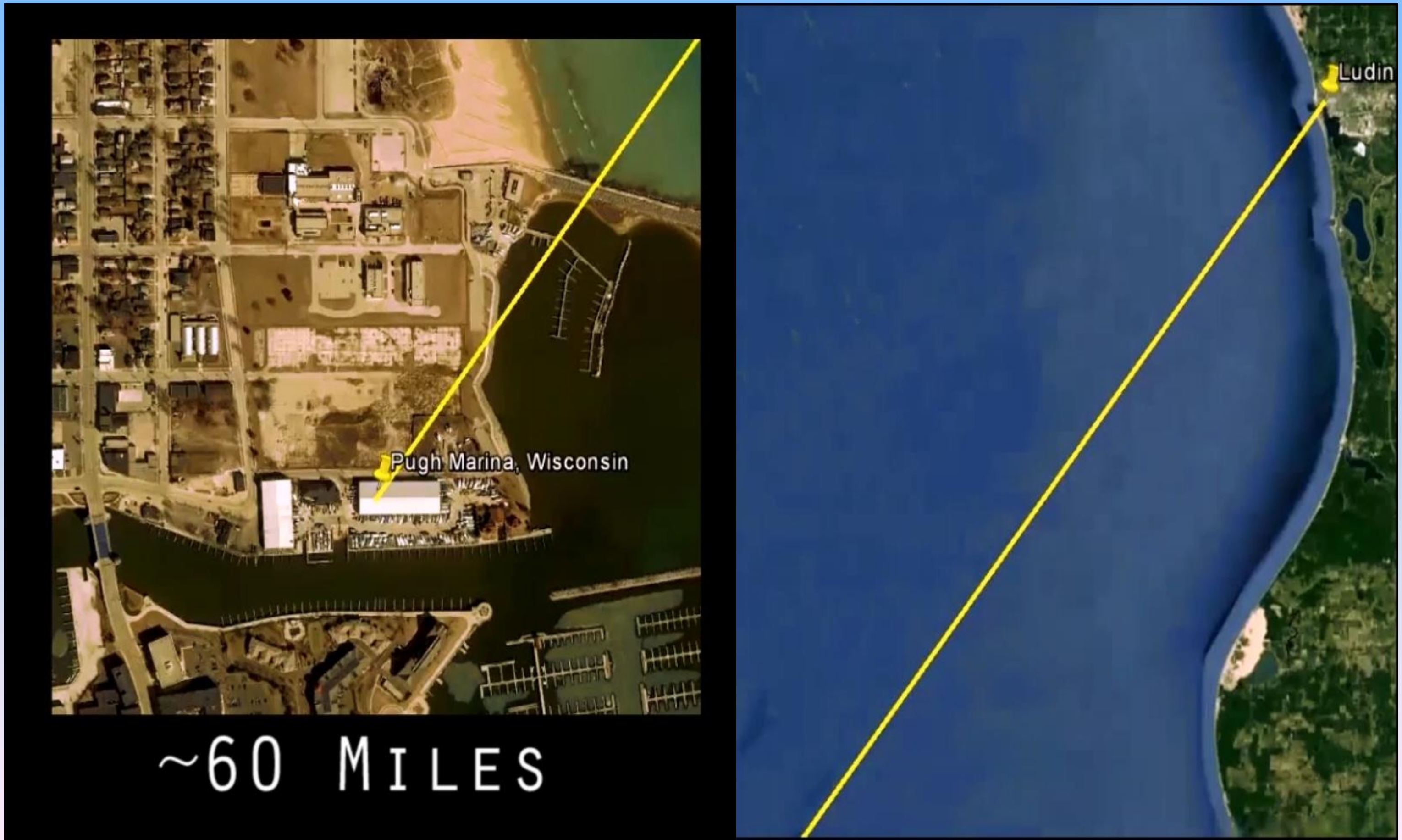


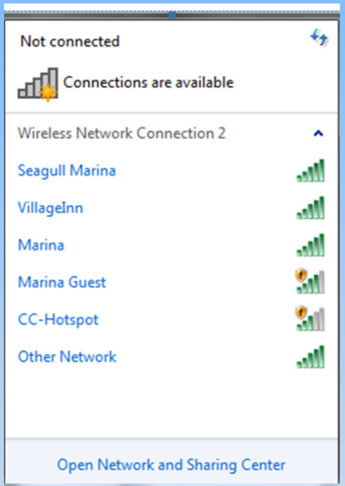
Drive disguised as a toy, hidden in a child's toy box that contained numerous images of CP

Wireless disk drive discovered during a raid that was hidden in a ceiling that contained numerous images of CP

How Far can a Wireless Network Signal Travel?

- How Far Does Your Wireless LAN Signal Extend?
  - Don’t Bet on it!





Not connected

Connections are available

Wireless Network Connection 2

Seagull Marina

VillageInn

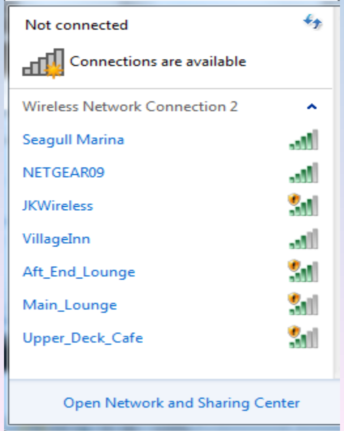
Marina

Marina Guest

CC-Hotspot

Other Network

Open Network and Sharing Center



Not connected

Connections are available

Wireless Network Connection 2

Seagull Marina

NETGEAR09

JKWireless

VillageInn

Aft_End_Lounge

Main_Lounge

Upper_Deck_Cafe

Open Network and Sharing Center

College Students Project Objective
(Presented at NGO Branch of U.N.)

- Compromise an internal network using:
  - Mobile devices
  - Specifically crafted applications
  - Social Engineering
  - Thumb drive storage
  - Concealment
  - Acquire information from five targeted systems in plain sight, without being visually or audibly detected and in less than 30 seconds.
  - Establish a covert channel to the Internet where they could download malicious software for compromising the internal network without being detected

Cyber Defense Research

Results

- The approach of influencing an employee to insert a benign version of a covert program was attempted four times within one organization with each attempt being successful.
- Another method involved having a person of unknown origin enter a server room of a community college and insert the same thumb drive into an operations server without being stopped or detected.
- The attempt was made and the device was inserted successfully and in plain sight of two individuals working in that room.

Egress of Stolen Information

- A targeted file representing confidential information was acquired from the target network.
- The acquired file was quickly embedded and hidden in the MP3 file using a Steganographic program downloaded from the Internet.
- The file was stored on a hidden thumb drive and concealed inside of a ball.
- The file exited the building in a bouncing ball, entered a vehicle and left the premises, all in plain sight.

Exercise the Compromise

- Students were then tasked with executing the monitoring and interception of a pre-compromised system on the target network from a remote location.

- The target system was compromised using the USB attack method previously demonstrated

- Within 10 minutes the mobile monitoring and was configured and in operation.

- Within five minutes of operation the target victim system was compromised and information acquired from it without detection by the user.

Results

- In each case if physical access was allowed to the room where the targeted computer was located, each system was successfully compromised.

- Additionally, this project begs the question that if college students can compromise an internal network without being detected, and with limited technical skill, then how deep into a corporate network could these same college students penetrate with some advanced training and a financial incentive.

Cyber Street Smarts - Do’s and Don’ts

-Drivers License Number – Derived from social media info!

-GPS info embedded into camera pics found on your social media site!

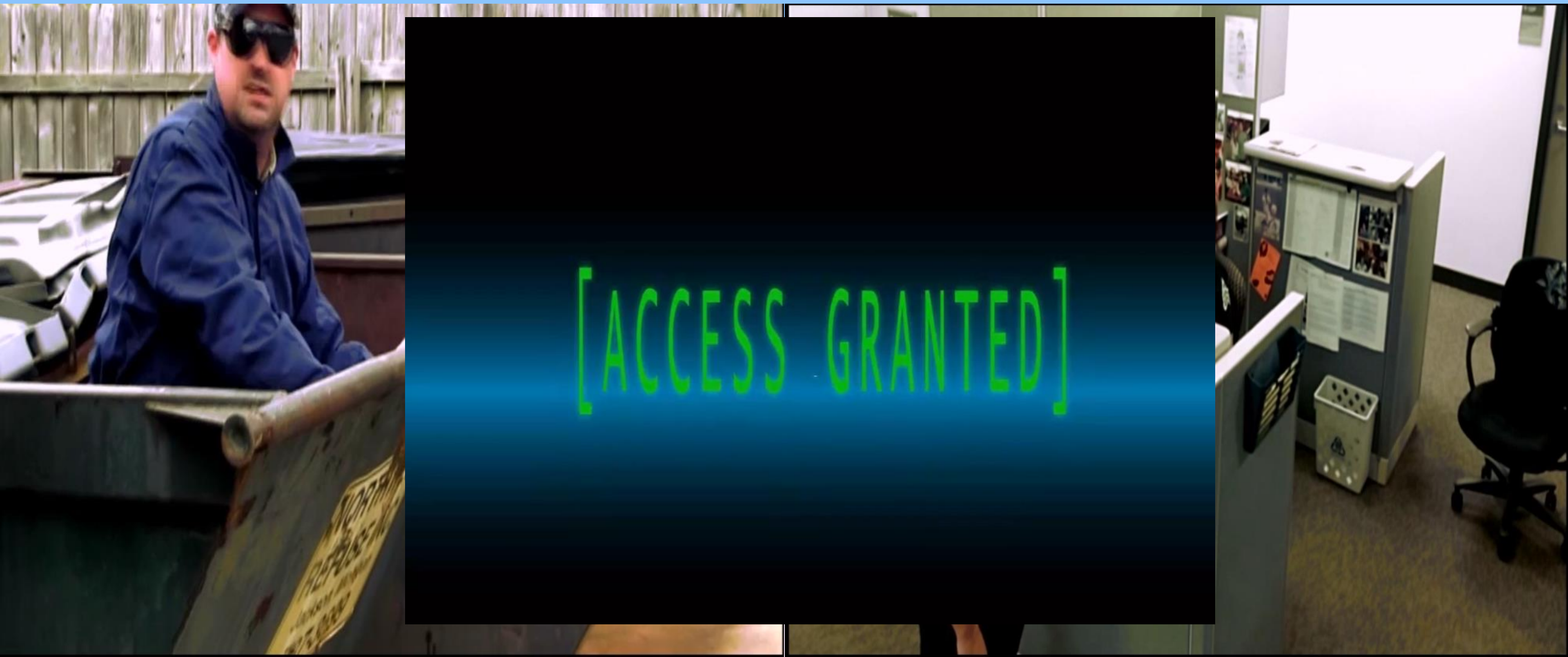
MICHIGAN
OPERATOR LICE
EXPIRE
Height
508
Eyes
GRY
Type
O
Endorsements
CY
NONE
M253112
Hacked
Your Full Name
+
Your Birth Month & Day
Your Driver's License Number

Cyber Street Smarts - Do’s and Don’ts

Turn off WiFi on your laptop when you are not using it!

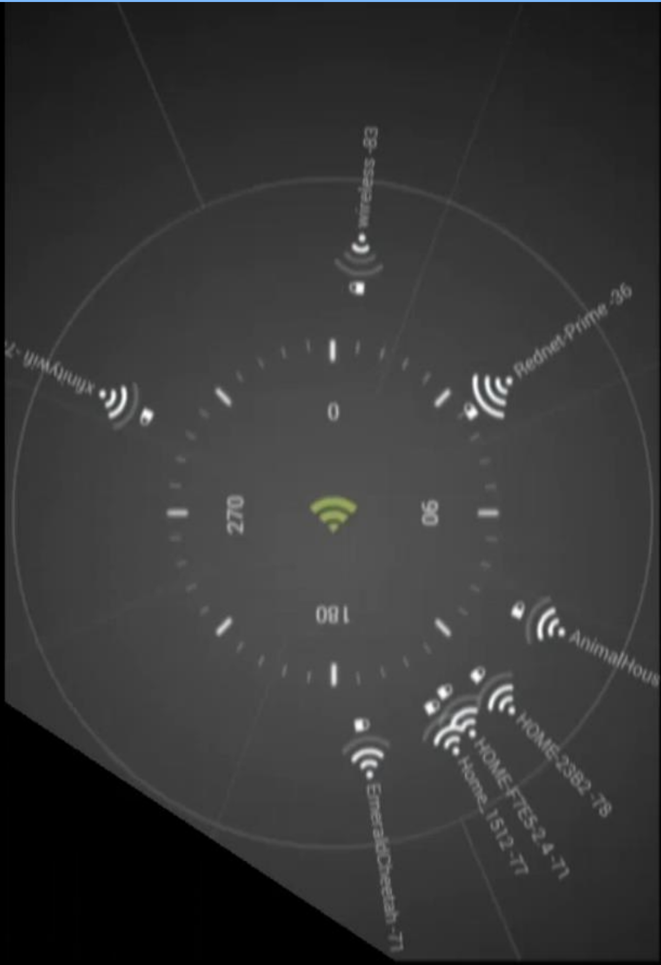
Cyber Street Smarts - Do’s and Don’ts

- NLP and social engineering – trick secretary into plugging into system or throwing something in trash!



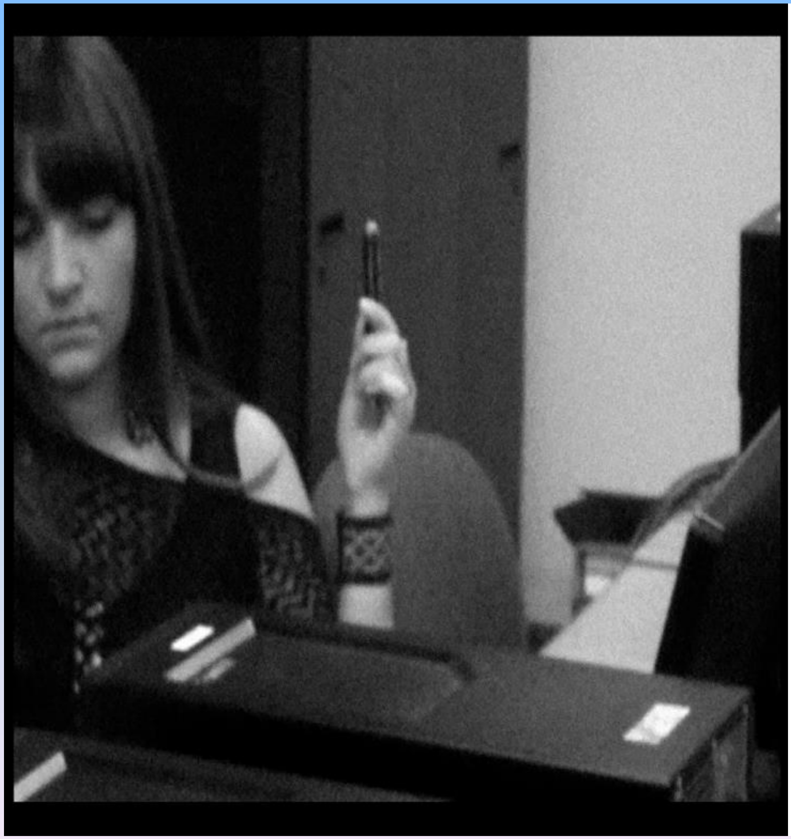
Cyber Street Smarts - Do’s and Don’ts

Detect cell phone probes then war drive with hi-gain antenna to track down a WiFi Beacon!



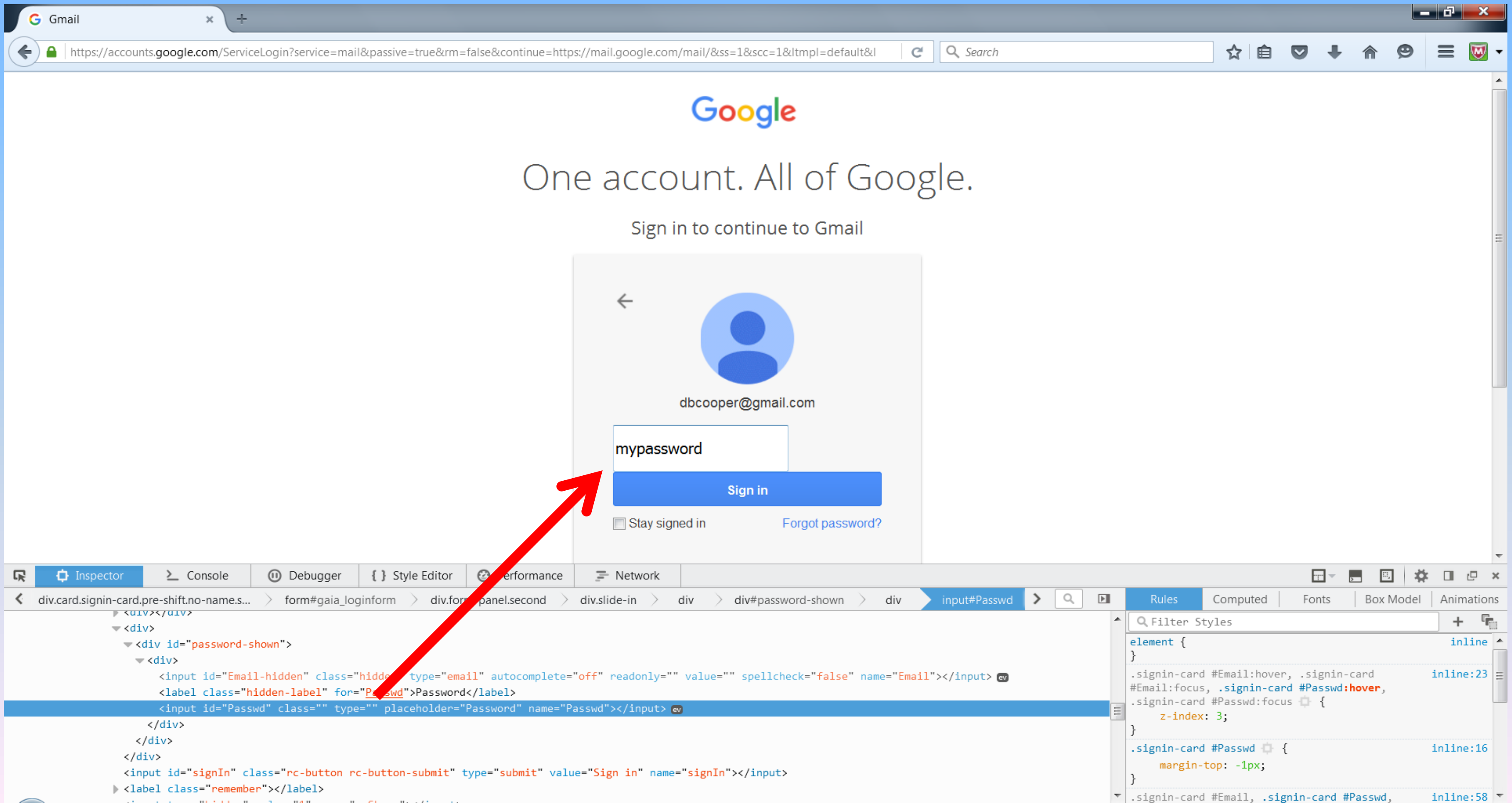
Cyber Street Smarts - Do’s and Don’ts

- Camera glasses and pens for reconnaissance



Cyber Street Smarts - Do’s and Don’ts

-Don’t leave browser logins unattended!



https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&scc=1&ltmpl=default&l

One account. All of Google.

Sign in to continue to Gmail

dbcooper@gmail.com

mypassword

Sign in

□ Stay signed in   Forgot password?

div.card.signin-card.pre-shift.no-name.s... > form#gaia_loginform > div.for panel.second > div.slide-in > div > div#password-shown > div > input#Passwd

```
    <div></div>
    <div>
      <div id="password-shown">
        <div>
          <input id="Email-hidden" class="hidde  type="email" autocomplete="off" readonly="" value="" spellcheck="false" name="Email"></input> ev
          <label class="hidden-label" for="P  swd">Password</label>
          <input id="Passwd" class="" type="" placeholder="Password" name="Passwd"></input> ev
        </div>
      </div>
    </div>
    <input id="signIn" class="rc-button rc-button-submit" type="submit" value="Sign in" name="signIn"></input>
    <label class="remember"></label>
```

```
element {                                                inline
}
.signin-card #Email:hover, .signin-card                  inline:23
#Email:focus, .signin-card #Passwd:hover,
.signin-card #Passwd:focus  {
    z-index: 3;
}
.signin-card #Passwd  {                                  inline:16
    margin-top: -1px;
}
.signin-card #Email, .signin-card #Passwd,               inline:58
```

Cyber Street Smarts - Do’s and Don’ts

- Do not store passwords on your computer!

  If you do, make them more than 15 characters
- Do not use public WiFi for confidential use: Wireless hi-jacking (Antenna)
- Do not insert unknown USB devices into your system!
- Erase files, don’t delete them!
- Metasploit tool allows for compromising anything!
- USB Capture –Windows command script, dump sam file, all information on system, then take back to hotel room or office to assess
- Thermal heat sensor on a cell phones?
- Windows Registry – Digital Truth Serum!
  - USB = serial number, make, model, date and time it was inserted
- If someone has physical access to your system, they own it!

- Demo reconnaissance info!

Six Points of Law and Technology

1. The use of information technology has transformed how countries are sustained

2. The use of information technology is blending cultures faster than anytime in history

3. The use of information technology is aligning those with similar suggestions and ideologies faster than anytime in history

4. The use of information technology has served as a catalyst for the advancement of every aspect of knowledge

5. No longer can users of information technology accept the risk that only their information is vulnerable in the event their system is compromised

6. The misuse of information technology is transforming law

J.A. Lewis

Real Time Threat Monitoring

- http://cybermap.kaspersky.com/
- http://map.ipviking.com/
- http://wwwnui.akamai.com/gnet/globe/index.html
- http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16349&view=map